# Congruences in Number Theory

Jonathan L.F. King
*University of Florida, Gainesville FL 32611-2082, USA*
squash@ufl.edu
Webpage http://squash.1gainesville.com/
4 April, 2021 (at *22:20*)

**Entrance.** Let Primes$(L)$ mean the <u>set</u> of primes that divide $L$. An ***arithmetic progression*** means a set $T + \mathbf{M}\mathbb{Z}$ of integers, where the ***gap*** (or ***modulus***) $\mathbf{M}$ is a posint and ***translation*** (or ***target***) $T$ an integer. Use ***comb***, also, for "arithmetic progression".

A comb $\mathcal{C} := T + \mathbf{M}\mathbb{Z}$ is ***coprime*** if $T \perp \mathbf{M}$.

## Divisibility Conundra

Here is a soln to LeVeque's #7 P.63: *Fix a coprime comb $\mathcal{C} := T + \mathbf{M}\mathbb{Z}$ and posint $L$. Prove there exists $x \in \mathcal{C}$ st. $x \perp L$.*

*Short solution.* Let $F$ be the maximum factor of $L$ such that $F \perp \mathbf{M}$. Letting $Q := \frac{L}{F}$, then,

1: $$\text{Primes}(Q) \subset \text{Primes}(\mathbf{M})\,.$$

Since $F \perp \mathbf{M}$, the CRT[♡1] applies to produce an integer $x$ with

2: $$x \equiv_{\mathbf{M}} T \quad\text{and}\quad x \equiv_F 1\,.$$

So in order to show that $x \perp L$, we need show that $x \perp Q$. FTSOC, suppose $p$ is a prime with $p \bullet\!| \; x$ and $p \bullet\!| \; Q$. This latter forces $p \bullet\!| \; \mathbf{M}$, by (??). Now LhS(??) forces $T \,|\!\bullet\, p$. This contradicts that $T \perp \mathbf{M}$. ♦

**Longer solution.** We use nested combs.

**3: Lemma.** *Fix a coprime comb $\mathcal{C} := T + \mathbf{M}\mathbb{Z}$. Each posint $L$ yields a coprime subcomb $\widehat{\mathcal{C}} \subset \mathcal{C}$, where*

∗: $$\widehat{\mathcal{C}} \;:=\; \widehat{T} + \widehat{\mathbf{M}}\cdot\mathbb{Z}\,, \quad \text{with } \widehat{\mathbf{M}} := \text{LCM}(\mathbf{M}, L).$$

*Proof.* Each integer $\widehat{T} \in \mathcal{C}$ is $\perp\mathbf{M}$ and defines a subcomb via (∗). So ISTProduce a $\widehat{T} \in \mathcal{C}$ with

¥: $$\widehat{T} \perp L\,,$$

for then, automatically, $\widehat{T}$ will be $\perp$LCM$(\mathbf{M}, L)$.

Consider $L = p_1{}^{k_1} \cdots p_K{}^{k_K}$, the prime factorization. If we find a $\widehat{T} \in \mathcal{C}$ coprime to $p_1 \cdots p_K$ then certainly $\widehat{T} \perp L$. So WLOG $\boxed{L \text{ is square-free}}$.

We'll now show that, WLOG,

£: $$\boxed{L \text{ is coprime to } \mathbf{M}.}$$

Letting $D := \text{GCD}(\mathbf{M}, L)$, necessarily, $\frac{L}{D} \perp \mathbf{M}$, since $L$ is square-free. And each $\widehat{T} \in \mathcal{C}$ is $\perp D$, so we just need to find one which is coprime to $\frac{L}{D}$.

Courtesy (£), we can pick a mod-$G$ reciprocal, call it $\beta$, of $L$. I.e, $\beta L \equiv_{\mathbf{M}} 1$. Our <u>goal</u> (¥) [we have a **yen** for it (…no, I'm *not* sorry)] is certainly satisfied by a $\widehat{T} \in \mathcal{C}$ with $\widehat{T} \equiv_N 1$. So we want an integer $y$ with

$$\widehat{T} \;:=\; 1 + Ny \overset{\text{Want}}{\in} \mathcal{C}\,,$$

i.e, with $1 + Ny \equiv_{\mathbf{M}} T$, i.e, with $Ny \equiv_{\mathbf{M}} T - 1$. It looks like $y := \beta[T-1]$ will do the trick. So we *define*

$$\widehat{T} \;:=\; 1 + N\beta[T-1]\,.$$

*Remark.* The above proof is entirely constructive. We actually could avoid the "square-free" step, at the cost of verbiage. □

**4: Very weak Dirichlet Thm[♡2].** *Each coprime comb $\mathcal{C} := T + \mathbf{M}\mathbb{Z}$ includes an infinite **pairwise coprime** subset $\{T_j\}_{j=1}^{\infty}$ of (distinct) integers.* ◊

*Proof.* Let $T_1 := T$ and $T_0 := \mathbf{M}$ and $\mathcal{C}_1 := T_1 + T_0\mathbb{Z}$. ISTProduce nested combs

$$\mathcal{C}_1 \supset \mathcal{C}_2 \supset \mathcal{C}_3 \supset \ldots \quad \text{of the form}$$
$$\mathcal{C}_j \;=\; T_j + [T_{j-1} \cdots T_1 \cdot T_0]\mathbb{Z}\,,$$

each a coprime comb.

Ok, at stage $j$, apply Lemma ?? to $\mathcal{C}_j$ with $N := T_j$. It hands us a translation amount $T_{j+1} := \widehat{T}$ which is coprime to

$$\text{LCM}(T_j, [T_{j-1} \cdots T_1 \cdot T_0]) \overset{\text{note}}{=\!=} T_j \cdot T_{j-1} \cdots T_1 \cdot T_0\,.$$

*Looks like a wrap, Folks.* ♦

[♡1] Chinese Remainder Thm: *Given arb. "targets" $s,t \in \mathbb{Z}$, $\exists x$ with $x \equiv_{\mathbf{M}} s$ and $x \equiv_F t$.*

[♡2] A much stronger result, Dirichlet's Theorem, asserts that every coprime comb includes infinitely many prime numbers.

**5: Two Comb Lemma.** *Two combs $\mathcal{C}_j := T_j + \mathbf{M}_j\mathbb{Z}$ intersect IFF*

$$\dagger\text{:}\qquad \mathrm{GCD}(\mathbf{M}_1, \mathbf{M}_2) \mathrel{\bullet\!\!\mid} [T_1 - T_2]$$

*Proof.* A integer $x$ is in $\mathcal{C}_1 \cap \mathcal{C}_2$ means there exist integers $z_i$ with $x + z_i\mathbf{M}_i = T_i$. Subtracting yields $z_1\mathbf{M}_1 - z_2\mathbf{M}_2 = T_1 - T_2$. This has a soln $(z_1, z_2)$ exactly when (†). When it does, use either $z_i$ to determine $x$. ♦

*Two remarks.* Suppose (†). The above gives an algorithm to compute an $x$. I call this ***fusing*** two (linear) congruences into a single congruence. Renaming this $x$ to $V$ and setting $L := \mathrm{LCM}(\mathbf{M}_1, \mathbf{M}_2)$, the algorithm fuses the pair $y \equiv_{\mathbf{M}_j} T_j$ of congruences, into a single $y \equiv_L V$ congruence.

The next result, the Pairwise-comb Thm, reminds me of Helly's theorem on convex sets. □

**6: Pairwise-comb Thm.** *Consider combs $\mathcal{C}_1, \ldots, \mathcal{C}_N$, where $\mathcal{C}_j := T_j + \mathbf{M}_j\mathbb{Z}$. Then the combs mutually intersect IFF each pair intersects. The non-void intersection $\bigcap_1^N \mathcal{C}_j$ has form $T + L\mathbb{Z}$, where $L$ is $\mathrm{LCM}(\mathbf{M}_1, \ldots, \mathbf{M}_N)$.*

*Since $x \in \mathcal{C}_j$ means*

$$Cj\text{:}\qquad x \equiv_{\mathbf{M}_j} T_j\,.$$

*Then the combs mutually intersect, producing a comb $T + L\mathbb{Z}$, where $L$ is $\mathrm{LCM}(\mathbf{M}_1, \ldots, \mathbf{M}_N)$.*

*Indeed, the combs mutually intersect IFF*

‡: *For each pair $j < k$ in $[1..N]$:* $\mathrm{GCD}(\mathbf{M}_j, \mathbf{M}_k) \mathrel{\bullet\!\!\mid} [T_j - T_k]$.

*Reduction.* Courtesy (**??**†), condition (‡) is necessary, so we will just show sufficiency.

It suffices to prove the $N$=3 case, since a simple induction on $N$ handles the general case. Considering a congruence $\boxed{\sigma\text{:}\ \ x \equiv_K S}$, our goal has become:

‡‡: *If each pair of (C1), (C2) and ($\sigma$) can fuse, then Fuse(C1,C2) can be fused with ($\sigma$).*

*Pf of (‡‡).* Write Fuse(C1,C2) as $x \equiv_L V$, where $L := \mathrm{LCM}(\mathbf{M}_1, \mathbf{M}_2)$. Thus each $T_j \equiv_{\mathbf{M}_j} V$. Hence $V - S \equiv_{\mathbf{M}_j} T_j - S$. With $\widehat{\mathbf{M}_j} := \mathrm{GCD}(\mathbf{M}_j, K)$, then,

$$V - S \equiv_{\widehat{\mathbf{M}_j}} T_i - S\,,$$

since $\widehat{\mathbf{M}_i} \mathrel{\bullet\!\!\mid} \mathbf{M}_i$. By hyp., (C$i$) and ($\sigma$) can fuse, i.e

$$T_i - S \equiv_{\widehat{\mathbf{M}_i}} 0\,,$$

Together, these give $[V - S] \mathrel{\mid\!\!\bullet} \widehat{\mathbf{M}_i}$. The upshot is

$$\mathrm{LCM}(\widehat{\mathbf{M}_1}, \widehat{\mathbf{M}_2}) \mathrel{\bullet\!\!\mid} [V - S]\,.$$

The last ingredient is that GCD distributes over LCM. Here,

$$\mathrm{GCD}(L, K) = \mathrm{LCM}(\widehat{\mathbf{M}_1}, \widehat{\mathbf{M}_2})\,.$$

Thus $\mathrm{GCD}(L, K)$ divides $[V - S]$, as desired. ♦

*Proof (unfinished).* ISTProve that the $N$ combs intersect. By induction on $N$, ISTEstablish the $N$=3 case.

Given three pairwise-intersecting combs, translate all three so that two intersect at the origin. So we may write these three combs as

$$7\text{:}\qquad A\mathbb{Z},\ \ B\mathbb{Z},\ \ T' + \mathbf{M}'\mathbb{Z}\,.$$

Let $D := \mathrm{GCD}(T', \mathbf{M}')$, $T := \frac{T'}{D}$ and $\mathbf{M} := \frac{\mathbf{M}'}{D}$. ISTFind a point

$$z \in AB\mathbb{Z} \cap [T + \mathbf{M}\mathbb{Z}]\,,$$

since then $zD$ is in each comb of (**??**).

So now $T \perp \mathbf{M}$. By hypothesis, Whoa! jk: Proof is broken. ♦

Filename: `Problems/NumberTheory/congruences.latex`
As of: *Saturday 04Mar2006.* Typeset: *4Apr2021 at 22:20.*